

UNITED STATES DISTRICT COURT

for the
Southern District of OhioRICHARD W. NAGEL
CLERK OF COURT

2019 JUN 21 AM 9:12

U.S. DISTRICT COURT
SOUTHERN DIST. OHIO

3:19mj341

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)SUBJECT DEVICES 1 THROUGH 3, IDENTIFIED IN
ATTACHMENT A

Case No.

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):
See Attachment A

located in the Southern District of Ohio, there is now concealed (identify the person or describe the property to be seized):
See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
18 U.S.C. 1924Offense Description
Unauthorized removal and retention of classified documents or material

The application is based on these facts:
See Attached Affidavit

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Sworn to before me and signed in my presence.

Date:

6/21/19

City and state: Dayton, Ohio

Brandt Pangburn

Applicant's signature

Brandt Pangburn, Special Agent

Printed name and title

Michael J. Newman

Judge's signature

Michael J. Newman, U.S. Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO

IN THE MATTER OF THE SEARCH OF
SUBJECT DEVICES 1 THROUGH 3,
IDENTIFIED IN ATTACHMENT A

Case No. _____

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Brandt Pangburn, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—electronic devices, namely a cellular phone, an external hard drive, and a laptop computer—which are currently in law enforcement possession, and which are described in Attachment A, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (“FBI”), Cincinnati Division, Dayton Resident Agency. I have been employed as a Special Agent with the FBI since July 2002. I have conducted national security and criminal investigations for the past 17 years and have received continuing training and education in all related matters. I have had specific experience and training in the proper handling and storage of classified material to include digital media. I possess a bachelor’s degree in Management Information Systems and worked in the computer industry for 9 years prior to joining the FBI.

3. As a federal agent, I am authorized to investigate violations of United States laws and to execute warrants issued under the authority of the United States.

4. The following information has been witnessed by me personally or has been conveyed to me by other law enforcement officers involved in the investigation of Izaak Vincent Kemp (hereinafter “Kemp”).

5. I have not included each and every fact known to me in this affidavit. I have only set forth the facts I believe are necessary to establish probable cause to believe that Kemp violated 18 U.S.C. § 1924, namely, unauthorized removal and retention of classified documents or material, and that evidence, fruits, and instrumentalities of this violation will be found on the identified electronic devices.

OVERVIEW OF CLASSIFIED INFORMATION HANDLING REQUIREMENTS

6. Under Executive Order 13526, information in any form may be classified if it: (1) is owned by, produced by or for, or is under the control of the United States Government; (2) falls within one or more of the categories set forth in the Executive Order [Top Secret, Secret, and Confidential]; and (3) is classified by an original classification authority who determines that its unauthorized disclosure reasonably could be expected to result in damage to the national security.

7. Pursuant to Executive Order 13526 § 1.2(a), information may be classified by the United States Government at one of three general levels: (1) “Top Secret” if the unauthorized disclosure of such information “reasonably could be expected to cause exceptionally grave damage to the national security;” (2) “Secret” if the unauthorized disclosure of such information “reasonably could be expected to cause serious damage to the national security;” or (3) “Confidential” if the unauthorized disclosure of such information “reasonably could be expected to cause damage to the national security.” Access to classified information at any level may

be further restricted through compartmentalization in Sensitive Compartmented Information (“SCI”) categories.

8. Generally, under Executive Order 13526 § 4.1, an individual may have access to classified information if: (1) a favorable determination of that individual’s eligibility for access has been made by an agency head or designee; (2) the individual has signed an approved nondisclosure agreement; (3) the individual has a need to know the information; and (4) the individual receives contemporaneous training on the proper safeguarding of classified information and on the criminal, civil, and administrative sanctions that may be imposed on any individual who fails to protect classified information from unauthorized disclosure. Individuals who meet these criteria and are granted access to classified information are commonly referred to as having a “security clearance” for information classified at a certain level.

9. Even if an individual possesses a security clearance, access to classified information at a certain level is allowed only if the individual possesses the clearance corresponding to that level of classification and the individual has a legitimate need to know the information. For example, an individual holding a security clearance for information classified at the “Secret” level is ineligible to access information classified at the “Top Secret” level. Moreover, even if that person requests access to information classified at the “Secret” level, access will be denied unless there is a legitimate need for that person to access the information as part of his or her duties.

10. 32 C.F.R. Parts 2001 and 2003 regulate the handling of classified information. Specifically, 32 C.F.R. § 2001.43, titled “Storage,” regulates the physical protection of classified information. This section prescribes that Secret and Top Secret information “shall be stored in a

GSA-approved security container, a vault built to Federal Standard (FHD STD) 832, or an open storage area constructed in accordance with § 2001.53.” It also requires periodic inspection of the container and the use of an Intrusion Detection System, among other things.

11. Classified information cannot be stored on or transferred using unclassified computers, servers, or internet service providers. Classified information must be maintained on devices specifically authorized by the U.S. government as authorized for classified information use. Individuals cannot use commercially available email providers, such as Gmail, Hotmail, or Yahoo, to transfer classified information. Classified information may be transferred using only U.S. government-approved closed networks. Classified material may not be stored in the homes of clearance holders.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

12. The property to be searched is: (1) a Samsung Galaxy Note 8 cellular telephone, with International Mobile Equipment Identity (IMEI) 358071084594927 (SUBJECT DEVICE 1); (2) a Hitachi 750GB external hard drive, with serial number 121210J1140021G3MNZJ (SUBJECT DEVICE 2); and (3) a Sony laptop Model PCG-61317L, serial number 275283393037702 (SUBJECT DEVICE 3) (collectively referred to as the “SUBJECT DEVICES”). The above-listed devices are currently located at the Evidence Control Room of the Dayton Resident Agency of the FBI, located in Centerville, Ohio, which is within the Southern District of Ohio.

13. The applied-for warrant would authorize the forensic examination of the SUBJECT DEVICES for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

14. Title 18, United States Code, Section 1924, provides that it is illegal for any officer, employee, contractor, or consultant of the United States, who, by virtue of his/her office, employment, position, or contract, becomes possessed of documents or materials containing classified information, to knowingly remove such documents or materials without authority and with the intent to retain such documents or materials at an unauthorized location.

15. On May 25, 2019, the Fairborn City Police Department executed a search warrant at Kemp's residence on 1231 Harmony Lane, Fairborn, Ohio 45324. The search was for evidence related to a marijuana growing facility believed to be located at Kemp's residence. During the search, officers found marijuana located at the residence.

16. Also found during the search of Kemp's residence were over 1000 pages of classified documents in paper form. An initial inspection of the documents revealed that they were clearly marked as classified. For example, many of the documents were marked with TOP SECRET at the top and bottom of the pages. The United States Air Force informed the FBI that the documents related to Top Secret Special Access Programs, meaning that they were restricted through compartmentalization in SCI categories.

17. Kemp is currently employed as a contractor at the U.S. Air Force National Air and Space Intelligence Center (NASIC) located at Wright Patterson Air Force Base in Fairborn, Ohio. He possesses a Top Secret security clearance. It is a violation of security policy to maintain Top Secret material outside of a secured and approved facility. It is also a violation of 18 U.S.C. § 1924 to knowingly remove such materials without authority and retain such materials at an unauthorized location. Kemp's personal residence is not an authorized location for the storage of classified information. According to the United States Air Force, Kemp was

never authorized to remove the above classified information from NASIC and would have had to make a concerted effort to bypass security checkpoints.

18. During a voluntary interview, which took place during execution of the search warrant, Kemp admitted to printing the classified materials at work and bringing them home for storage.

19. Kemp gave the interviewing Agents consent to take possession of a laptop, a cell phone, and an external hard drive found at the residence (the SUBJECT DEVICES). Kemp signed an FBI consent to search form and the interviewing Agents took possession of the items and stored them as evidence in the Dayton FBI Evidence Room. Notwithstanding Kemp's consent, a search warrant is being sought for these devices out of an abundance of caution.

20. Kemp is known to work on computers as part of his duties at NASIC and reported to interviewing Agents that the classified documents found at his residence were printed from U.S. Air Force computers.

21. The SUBJECT DEVICES are currently in storage at the Evidence Control Room located at the Dayton Resident Agency of the FBI in Centerville, Ohio. In my training and experience, I know that the devices have been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when the devices first came into the possession of the FBI.

22. Based on the information above, I submit that there is probable cause to believe that Kemp has committed violations of Title 18, United States Code, Section 1924, and that evidence, fruits, and instrumentalities of those violations will be present on the SUBJECT DEVICES. As discussed above, this investigation has revealed that Kemp stored classified Top Secret documents at his residence that he printed from government computers. Based on my

training and experience, I know that classified information is often stored and accessed in electronic form on computers, hard drives, and other electronic media and devices. I also know that classified information can be electronically transferred to and from such electronic devices. Further, I know based on my training and experience that individuals involved in counterintelligence offenses often use mobile telephone devices and forms of electronic communication to communicate with others about such offenses.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

23. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

24. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the devices were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the devices because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.
- f. I know that when an individual uses an electronic device to communicate with individuals believed to be members of a foreign intelligence service, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain:

data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.


25. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the devices to human inspection in order to determine whether it is evidence described by the warrant.

26. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

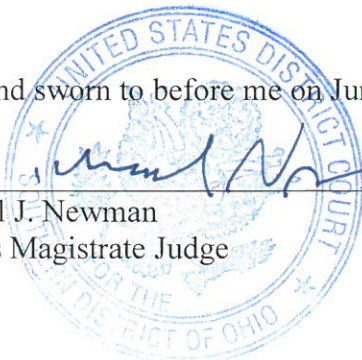
27. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the devices described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,


Brandt Pangburn
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on June 21, 2019.


Hon. Michael J. Newman
United States Magistrate Judge



ATTACHMENT A

The property to be searched is: (1) a Samsung Galaxy Note 8 cellular telephone with International Mobile Equipment Identity (IMEI) 358071084594927 (SUBJECT DEVICE 1); (2) a Hitachi 750 GB hard drive with serial number 121210J1140021G3MNZJ (SUBJECT DEVICE 2); and (3) a Sony laptop computer model number PCG-61317L with serial number 275283393037702 (SUBJECT DEVICE 3). All of the above devices are currently located at the FBI's Dayton Resident Agency in Centerville, Ohio.

This warrant authorizes the forensic examination of the devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Subject Devices described in Attachment A that relate to violations of 18 U.S.C. § 1924, including but not limited to:
 - a. Email, text and other messages, photos, videos, contacts and contact lists, addresses and address books, voicemail messages, dialed calls, incoming calls, received calls, outgoing calls, location data, calendar, applications and application data, settings;
 - b. Records and information relating to any classified information;
 - c. Records and information relating to the unauthorized transfer of any U.S. Air Force information;
 - d. Records and information relating to travel, including travel plans, itineraries, reservations, bookings, tickets, and the means and sources of payment for travel;
 - e. Records and information relating to intentions, attempts, and plans to provide U.S. Air Force information to unauthorized persons or entities;
 - f. Records and information relating to communications with other individuals associated with foreign intelligence services, their surrogates, co-conspirators, accomplices, and associates;
 - g. Records and information relating to Kemp's use of YouTube, Facebook, messaging applications, and other forms of social media and internet communication, including private messaging;
 - h. Identifying and contact information of co-conspirators and other individuals engaged or otherwise involved in the unauthorized possession of classified material.

- i. Evidence of who used, owned, or controlled the devices at the time things described in the warrant were created, edited, deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
- j. Evidence of software that would allow others to control the Device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- k. Evidence of the lack of such malicious software;
- l. Evidence indicating how and when the devices were accessed or used to determine chronological context of access, use, and events relating to crime under investigation and to the Device user;
- m. Evidence indicating the devices user’s state of mind as it relates to the crime under investigation
- n. Evidence of attachment to the devices of other storage devices or similar containers for electronic evidence;
- o. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the devices;
- p. Evidence of times the devices was used;
- q. Passwords, encryption keys, and other access devices that may be necessary to access the Device;

- r. Documentation and manuals that may be necessary to access the devices or to conduct a forensic examination;
- s. Records and information about Internet Protocol addresses used by the devices;
- t. Records and information about the devices' Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and,
- u. Contextual information necessary to understand the evidence described in this attachment.

2. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.